Listing of Claims:

1. (Previously Presented) A method of accessing a service with authentication and revocable anonymity, comprising the steps of:

i) identifying and registering a client and providing the client with means for authenticating the client to an anonymous certification authority;

ii) authenticating the client to the anonymous certification authority using the means provided in step i) and supplying the client with an anonymous certificate associated to a public key and configured to enable the client to authenticate the client anonymously to a server;

iii) the client calculating data formed as a series of tokens, wherein an initialization token of the series of tokens is configured to enable an authentication session to be opened and tokens of the series of tokens other than the initialization token are configured to enable the authentication session to be maintained;

iv) authenticating the client by producing an anonymous signature of the initialization token, the signatures being obtained using a private key associated with said public key and opening an anonymous authentication session with the server, wherein said anonymous signature is a unique signature used for said authentication session;

v) maintaining the anonymous authentication session with the aid of the series of tokens, thereby enabling the server to prove each of the actions of the client; and

vi) selectively allowing contact between the server and the anonymous certification authority to revoke the anonymity of the client using the anonymous signature provided in step iv.

2. (Previously Presented) The method according to claim 1, further comprising: effecting communication between the anonymous certification authority and the server, before the authenticating of the client to the anonymous certification authority, whereby the server presents to said anonymous certification authority a request to obtain means enabling verification of the anonymous authentication supplied by a client.

3. (Canceled)

4. (Previously Presented) The method according to claim 1, wherein each of the tokens of the series of tokens is configured for one-time use and each of the tokens of the series of tokens is strongly interdependent.

5. (Previously Presented) The method according to claim 1, wherein the tokens of the series of tokens are calculated using two cryptographic primitives.

6. (Previously Presented) The method according to claim 4, wherein a first token W_i of the series of tokens is obtained by applying a hashing function H to a random number, a second token W_z of the series of tokens is obtained by applying the hashing function to the first token obtained, and so on until a token of rank n of the series of tokens defines the initialization token W_n as:

$$H(W_0)=W_1 H(W_{n-1})=W_n.$$

7. (Canceled)

8. (Canceled)

9. (Previously Presented) The method according to claim 6, wherein on each new authentication the client sends the server a token of the series of tokens of at least one unit lower rank than that previously used.

10. (Previously Presented) The method according to claim 6, wherein on each new authentication the client sends the server a token W_i of the series of tokens whose rank (i) is representative of a value of an operation.

11. (Previously Presented) The method according to claim 6, wherein the steps are applied to bidding and steps of the client submitting an increased bid are effected by sending successive tokens of lower rank.

12. (Previously Presented) The method according to claim 1, further comprising using a group signature by associating a plurality of identifiers and respective private keys with a single group public key.

13. (Previously Presented) The method according to claim 1, wherein the anonymous signature is a blind signature.

14. (Previously Presented) The method according to claim 12, wherein a power to revoke anonymity is shared between two or more authorities.

15. (Currently Amended) A system adapted to open and maintain an authentication session guaranteeing non-repudiation, wherein an anonymous signature unique to the session and comprising a series of tokens is used to open and maintain each session, the system comprising:

means for implementing three stages comprising:

a first stage in which a client calculates the series of tokens, an initialization token of the series of tokens being configured to enable the authentication session to be opened and another token of the series of tokens being configured to enable the authentication session to be maintained;

a second stage in which the client makes a strong undertaking to the server as to the series of tokens; and

a third stage of maintaining the anonymous authentication session with the aid of the series of tokens, thereby enabling the server to prove each action of the client,

wherein a client is authenticated by producing the anonymous signature of the initialization token, the signatures being obtained using a private key associated with a public key and opening the authentication session with a server.

16. (Previously Presented) The system according to claim 15, wherein the first stage calculates the series of tokens based on two cryptographic primitives, wherein the two cryptographic primitives are a hashing function and a random number.

17. (Currently Amended) The system according to claim 15, wherein the system is configured to use a group signature by associating a plurality of identifiers and respective private keys with the public key being a single group public key.

18. (Previously Presented) The system according to claim 15, wherein the unique anonymous signature is a blind signature.

19. (Previously Presented) The system according to claim 15, wherein power to revoke anonymity is divided between two or more authorities.

20. (Previously Presented) The method according to claim 5, wherein the two cryptographic primitives are a hashing function and a random number.

21. (Previously Presented) The method according to claim 10, wherein the rank is representative of a number of bid increments.